Claims

1. A method of detecting suspicious electronic messages (101, 102, 103), wherein the method is performed in a messaging server (1000) which is in communication with a plurality of message senders (110-110m) and a plurality of message receivers (120-120k), wherein the method comprises the steps of:

receiving electronic messages (101, 102, 103) sent from the plurality of message senders (110-110m) to at least one message receiver (120-120k);

extracting from each received message (101, 102, 103) at least one message sender feature (AF) and at least one message content feature (CF);

recording the extracted at least one message sender feature (AF) and at least one message content feature (CF) in a database (1060);

determining, on the basis of the message content features (CFs) recorded in the database (1060), whether a specific content feature that can be associated with a current message (101) has already been recorded in the past;

if the specific content feature has already been recorded in the past, determining, on the basis of the message sender features (AFs) recorded in the database (1060), a number (N) of message senders (110-110m) that can be associated with the specific content feature; and

classifying the current message (101) as suspicious if the determined number (N) of message senders (110-110m) that can be associated with the specific content feature exceeds a predetermined threshold value (N1).

2. The method according to claim 1, further comprising generating timestamps (ts) and recording the timestamps (ts) along with the extracted message sender features (AFs) and message content features (CFs) in the database (1060).

3. The method according to claim 2, wherein the recording step further comprises: organizing the time-stamped message sender features (AFs) and message content features (CFs) into at least one index data structure (IDX1, IDX2).

4. The method according to claim 3, wherein the time-stamped message sender features (AFs) and message content features (CFs) are recorded in two separate index data structures, wherein a first index data structure (IDX1) comprises a data set (ts, CF) of time-stamped message content features (CFs) and a second index data structure (IDX2) comprises a data set (ts, CF, AF) of time-stamped message content features (CFs) and message sender features (AFs).

5. The method according to any one of the preceding claims, wherein the step of determining whether specific content features has already been recorded in the database (1060) comprises:

performing an identity or similarity check between the message content feature (CF) associated with the current message (100) and the recorded message content features (CFs) in the database (1060).

6. The method according to claim 5, wherein a database look-up is performed in order to determine whether a content feature record identical or similar to the specific content feature already exists in the database (1060) for a predetermined time window in the past.

7. The method according to claim 5 or 6, wherein if a message content feature record identical or similar to the specific content feature already exists in the database (1060) for a predetermined time window, determining how many message sender features (AFs) can be related to the existing content feature record for the predetermined time window.

8. The method according to any one of the preceding claims, wherein the classifying step further comprises at least one of the following processes:

tagging the current message (101) as suspicious message; and

registering the content of the current message (101) as spam or malicious content in a blacklist.

9. The method according to any one of the preceding claims, wherein if the current message (101) has been classified as suspicious, the method further comprising at least one of the following steps:

blocking the current message (101); and

subjecting the current message (101) to an AV analysis.

10. The method according to claim 9, further comprising:

routing the current message (101) to the intended message receiver (120-120k) if the AV analysis reveals that the message (101) is not malicious.

11. The method according to any one of the preceding claims, wherein the at least one extracted message sender feature (AF) is indicative of a sender address or sender address portion.

12. The method according to any one of the preceding claims, wherein the at least one extracted message content feature (CF) is indicative of an attachment of the message, subject line content of the message, URL comprised in the message and/or portions thereof.

13. A computer program product comprising program code portions for carrying out the method according to any one of the preceding claims, when the computer program product is executed on a computer device.

14. The computer program product according to claim 13, the computer program product being stored on a computer-readable recording medium.

15. A messaging server (1000) for detecting suspicious electronic messages (101, 102, 103), wherein the messaging server (1000) is in communication with a plurality of message senders (110-110m) and a plurality of message receivers (120-120k), the messaging server (1000) being configured to receive electronic messages (101, 102, 103) sent from the plurality of message senders (110-110m) to at least one message receiver (120-120k), the server (1000) comprising:

an analysing unit (1010) configured to extract at least one message sender feature (AF) and at least one message content feature (CF) from each received message (101, 102, 103);

a recording unit (1030) configured to record the extracted at least one message sender feature (AF) and at least one message content feature (CF) in a database (1060);

a determining unit (1040) configured to determine, on the basis of the message content features (CFs) recorded in the database (1060), whether a specific content feature that can be associated with a current message (101) has already been recorded in the past, and if the specific content feature has already been recorded in the past, to further determine, on the basis of the message sender features (AF) recorded in the database (1060), a number (N) of message senders (110-110m) that can be associated with the specific content feature; and

a classifying unit (1050) configured to classify the current message (101) as suspicious if the determined number (N) of message senders (110-110m) that can be associated with the specific content feature exceeds a predetermined threshold value (N1).

16. The messaging server according to claim 15, further comprising a time-stamping unit (1020) configured to provide a timestamp (ts) for each extracted message sender feature (AF) and message content feature (CF).